Metodisk tilnærming til vurdering av personvernkonsekvenser

Finans Norge september 2020

Cecilie Rønnevik

Advokat/direktør i Advokatfirmaet PricewaterhouseCoopers

Noen utgangspunkter

Formålet med vurderingene

Å identifisere om det må iverksettes *ytterligere vilkår eller begrensninger* enn det som følger av de alminnelige bestemmelsene i GDPR

Konsesjonsordningen etter personopplysningsloven 2001 §§ 34 og 35

"*Ved avgjørelse av om konsesjon kan gis skal det klarlegges om behandlingen av personopplysninger kan volde ulemper for den enkelte som ikke avhjelpes gjennom bestemmelsene i kapitlene II-V*" (de alminnelige vilkårene)

"*I konsesjonen skal det vurderes å sette vilkår for behandlingen når slike vilkår er nødvendige for å begrense ulempene …*"

Et typisk tilleggsvilkår var at den behandlingsansvarlige måtte bekrefte regelmessig til Datatilsynet at behandlingen skjedde i samsvar med konsesjonen. Det ble også lagt begrensninger for behandlingen, f eks sletting.

De alminnelige bestemmelsene er skjønnsmessige

De gir tilstrekkelig vern i de fleste tilfeller

Det er rent *unntaksvis* nødvendig med ytterligere vilkår eller begrensninger

Likevel en erkjennelse av at de alminnelige bestemmelsene ikke nødvendigvis strekker til i alle sammenhenger

Gjenstanden for vurderingene

Behandlingsaktiviteter

En eller flere

Identifisert ved et (felles) *konkret* behandlingsformål, feks:

- rekruttering
- direkte markedsføring
- utarbeide konkrete tilbud
- osv

Informasjonssystemer

Er som sådan *ikke* gjenstand for DPIA, men

- skal alltid risikovurderes, jf art. 32
- er relevant når risikoen ved behandlingsaktivitetene skal vurderes
  - endringer i systemene kan medføre behov for (ny) DPIA

Unntak

Den behandlingsansvarlige skal ikke overprøve de personvernkonsekvensvurderinger som er gjort av lovgiver (art. 35 nr. 10)

Rettslig grunnlag

Behandlingen er nødvendig for å

- Oppfylle en rettslig forpliktelse, jf. art. 6 nr. 1 bokstav c
- Utøve offentlig myndighet, jf. art. 6 nr. 1 bokstav e

Supplerende rettsgrunnlag

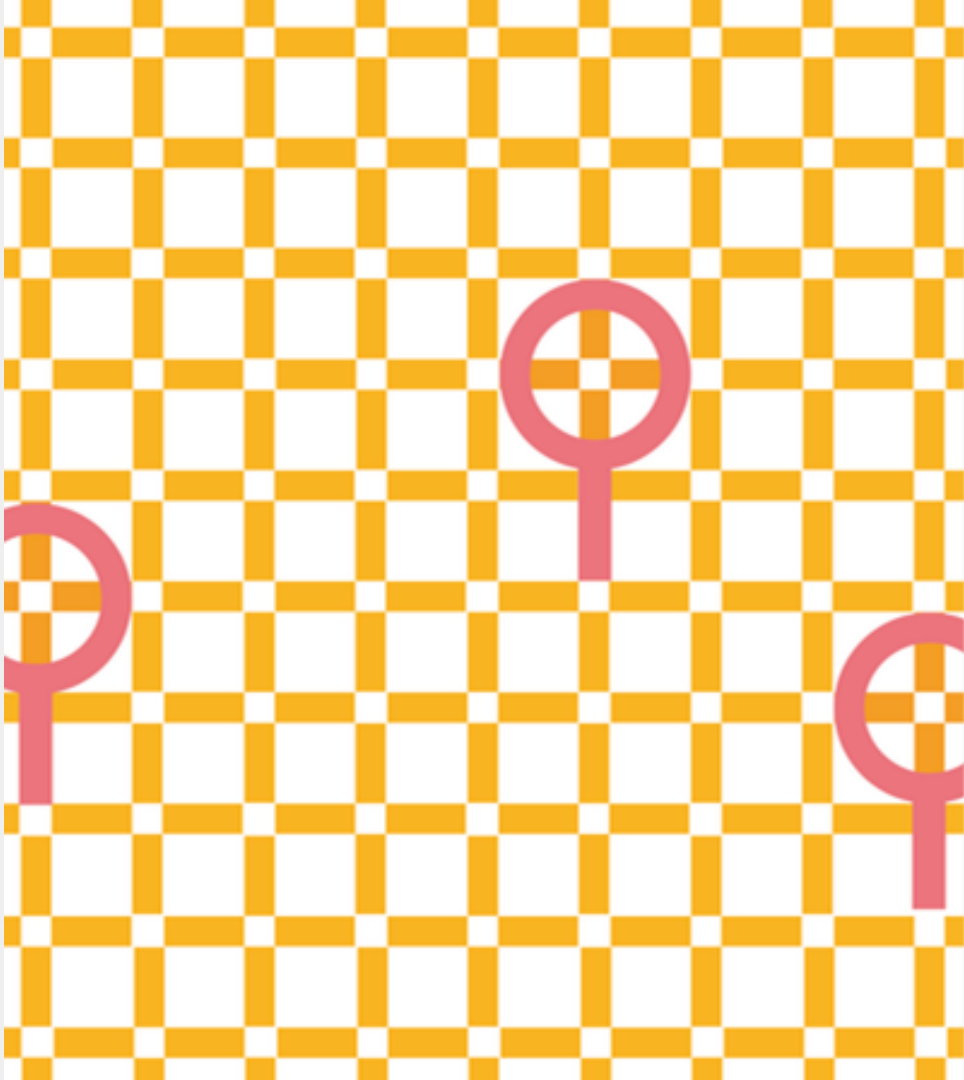
Grunnlaget for behandlingen er fastsatt i unionsretten eller medlemsstatens nasjonale rett som den behandlingsansvarlige er underlagt.

Lovgiver har vurdert personvern-konsekvensene

I forbindelse med vedtakelse av de nasjonale bestemmelsene

https://www.regjeringen.no/no/dokumenter/vurdering-av-personvernkonsekvenser/id533574/

1 Legg planer for å etterleve de alminnelige bestemmelsene, art. 24



Planene må være så *konkrete* at det er mulig å vurdere om det gir tilstrekkelig vern, men likevel være så *foreløpige* slik at det er rom for endringer

Planlegg behandlingen

- Behandlingsaktiviteten(e)
- Formålet med behandlingen(e)
- Kategorier av registrerte
- Kategorier av personopplysninger
- Konteksten behandlingen skal skje i
- Berettigede forventninger
- Rettslig grunnlag for behandlingen
- Osv

Planlegg tekniske og organisatoriske tiltak for å sikre etterlevelse

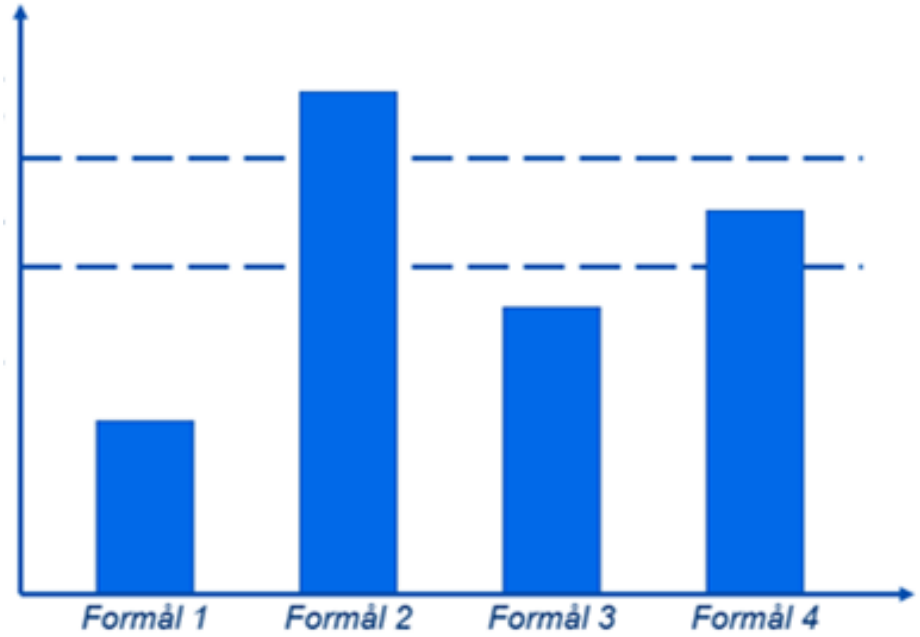
- Ansvarsplassering
- Tiltak for å sikre rettslig grunnlag
- Tiltak for å gi informasjon
- Tiltak for at de registrerte enkelt skal kunne henvende seg
- Tiltak for å slette opplysningene
- Osv

Risikonivå

Høy restrisiko

Høy risiko

Alminnelig risiko



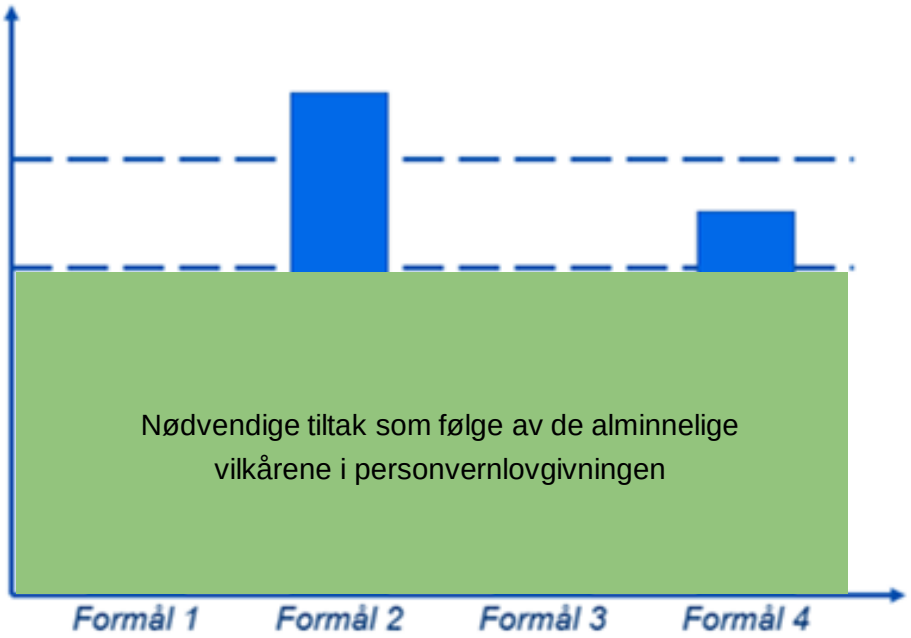
Behandlingsaktivitet

Risikonivå

Høy restrisiko

Høy risiko

Alminnelig risiko



Alminnelige vilkår, jf GDPR art. 24 mv.

Behandlingsaktivitet

2 Vurder om det er høy risiko, art. 35

Utgjør behandlingen en risiko for fysiske personers rettigheter og friheter, *til tross for at personvernforordningens alminnelige bestemmelser er fulgt*?

Identifisere mulige konsekvenser for rettigheter og friheter

- også utover rett til privatliv og personopplysningsvern
- også positive konsekvenser
- også for andre fysiske personer enn de registrerte

Vurdere sannsynligheten for at konsekvensene faktisk oppstår

Høy risiko antas å foreligge i visse typetilfeller

- Oppramsing i GDPR art. 35
- Veileder fra EDPB http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
- Veileder fra Datatilsynet https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/

3 Vurder endringer i de opprinnelige planene, art. 35

Hvis det foreligger høy risiko må man vurdere hvilke endringer som er *egnet* til å begrense den aktuelle risikoen

Endringer i behandlingsmåten

- Begrense opplysningstyper eller kategorier registrerte - *selv om* man har rettslig grunnlag
- Unnlate overføring til tredjeland - *selv om* man har overføringsgrunnlag
- Annet som går *ut over* alminnelige vilkår iGDPR

Ytterligere tekniske og organisatoriske tiltak

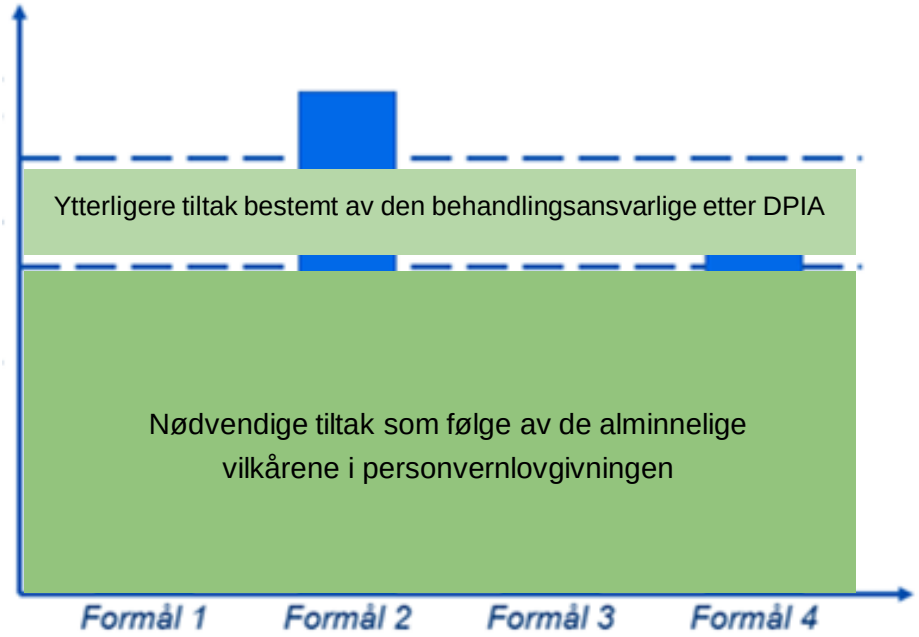
- Etablere personvernombud - *selv om* man ikke plikter
- Informere de registrerte - *selv om* man har unntak (og det ikke er forbudt)
- Å gi de registrerte adgang til å protestere, selv om det ikke er pålagt
- Annet som går *ut over* alminnelige vilkår

Risikonivå

Høy restrisiko

Høy risiko

Alminnelig risiko

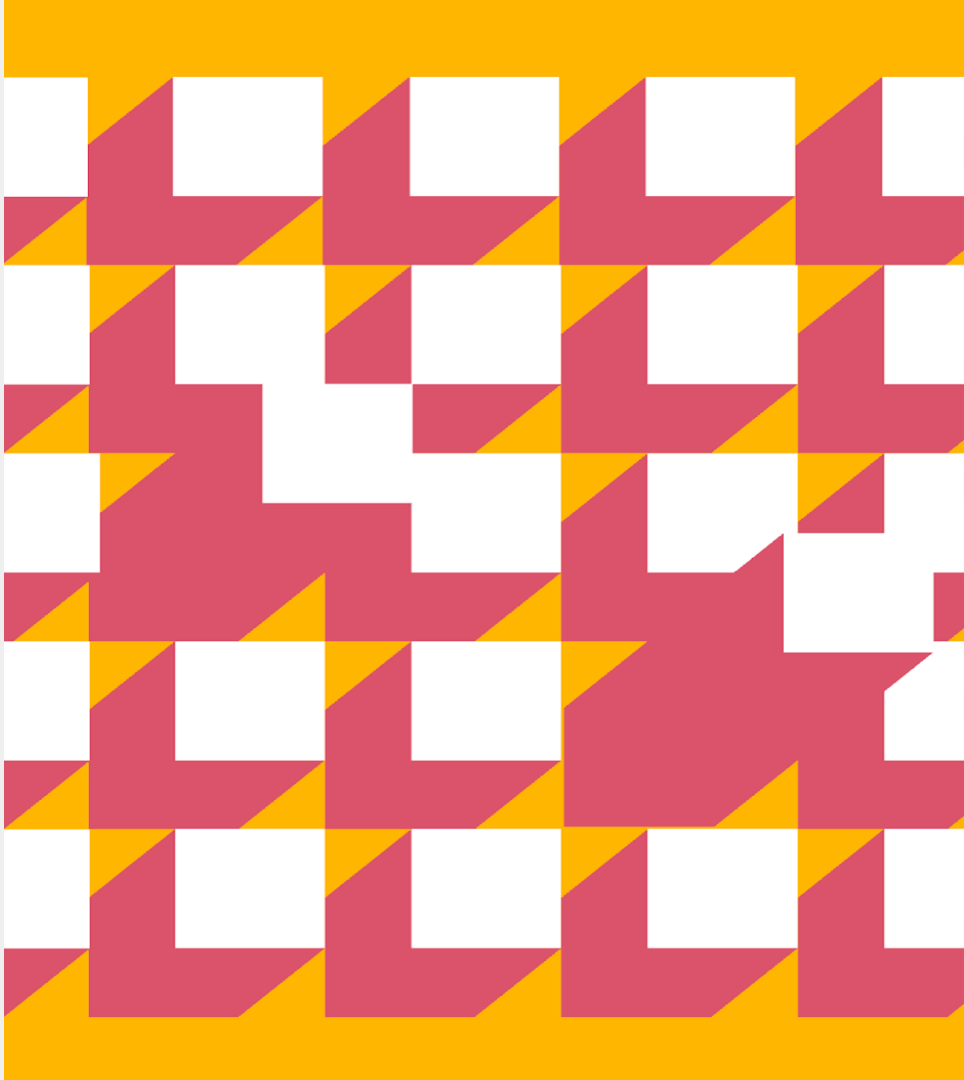


GDPR art. 35

GDPR art. 24

Behandlingsaktivitet

3 Vurder om det er restrisiko, jf art. 36



Utgjør behandlingen fremdeles en risiko, til tross for at det gjøres *ytterligere tiltak eller begrensninger* for å sikre rettigheter og friheter?

Alt. 1 Forhåndsdrøftelse

- Datatilsynet mener risikoen allerede er akseptabel, gitt tiltakene
- Datatilsynet foreslår ytterligere tiltak eller endringer
- Datatilsynet utsteder er advarsel om at de planlagte aktivitetene er i strid med forordningen
- Datatilsynet pålegger endringer eller opphør av behandlingen (hvis igangsatt)

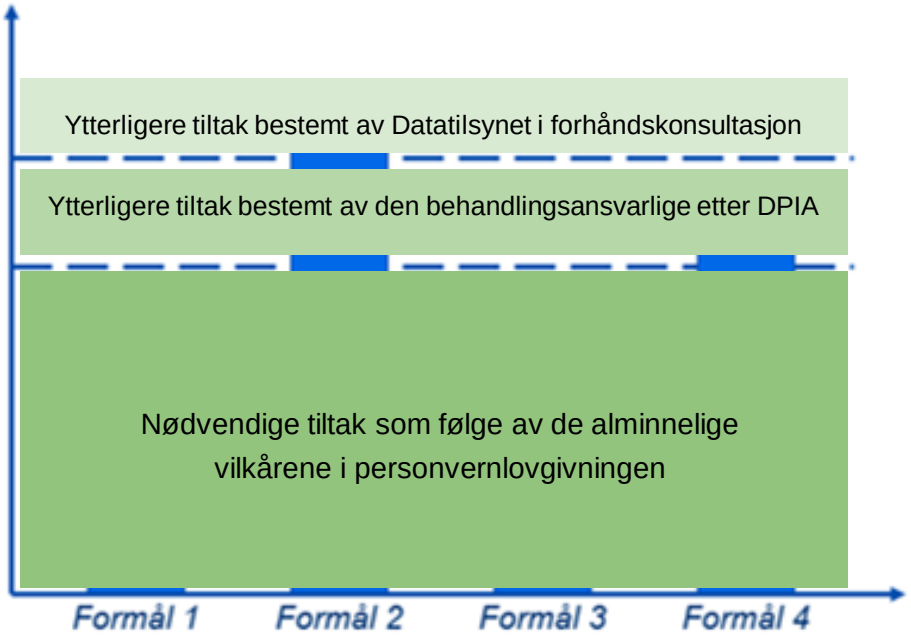
Alt 2. Endringer eller stans

Risikonivå

Høy restrisiko

Høy risiko

Alminnelig risiko



GDPR art. 36

GDPR art. 35

GDPR art. 24

Behandlingsaktivitet

Konsekvenser av å ikke gjøre DPIA

Manglende vurderinger

Er i seg selv et brudd på forordningen

Brudd på art. 35 og 36 kan sanksjoneres iht art. 83 nr. 4 bokstav med gebyr på inntil 10 mill euro

Manglende tiltak

Kan innebære brudd på de grunnleggende prinsippene i art. 5

Selv om de alminnelige bestemmelsene i forordningen etterleves.

Brudd på art. 5 er selvstendig grunnlag for gebyr iht art. 83 nr. 5 med inntil 20 mill euro

Oppsummering

Begynn med å sikre etterlevelse av de alminnelige vilkårene i forordningen

Vurder behandlings-aktiviteter

Sørg for at en evt DPIA oppfyller formålet om å identifisere behovet for ytterligere tiltak

Datatilsynet har alminnelig veiledningsplikt

Takk for meg!

Cecilie Rønnevik

PwC | Direktør I Senioradvokat

Mobil: +47 91 39 34 36
E post: cecilie.ronnevik@pwc.com
Advokatfirmaet PricewaterhouseCoopers AS,

Dronning Eufemias gate 71, 0191 Oslo
P.O. Box 748, Sentrum, NO-0106 Oslo

http://www.pwc.no

pwc.com